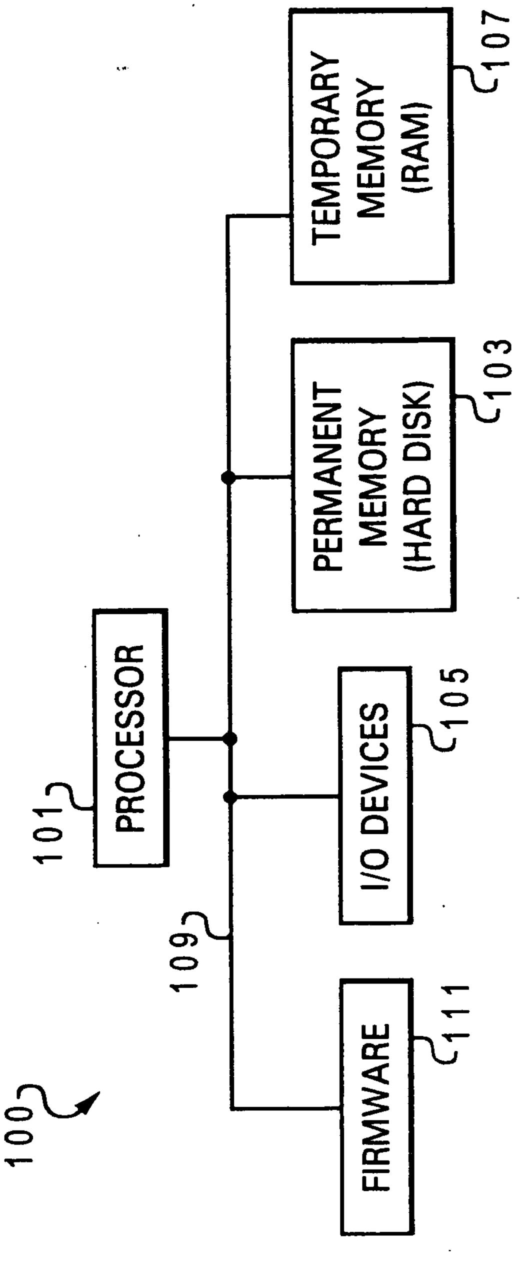

TEMPORARY MEMORY (RAM)
107
PERMANENT MEMORY (HARD DISK)
103
PROCESSOR
101
I/O DEVICES
105
109
FIRMWARE
111
100

Fig. 1

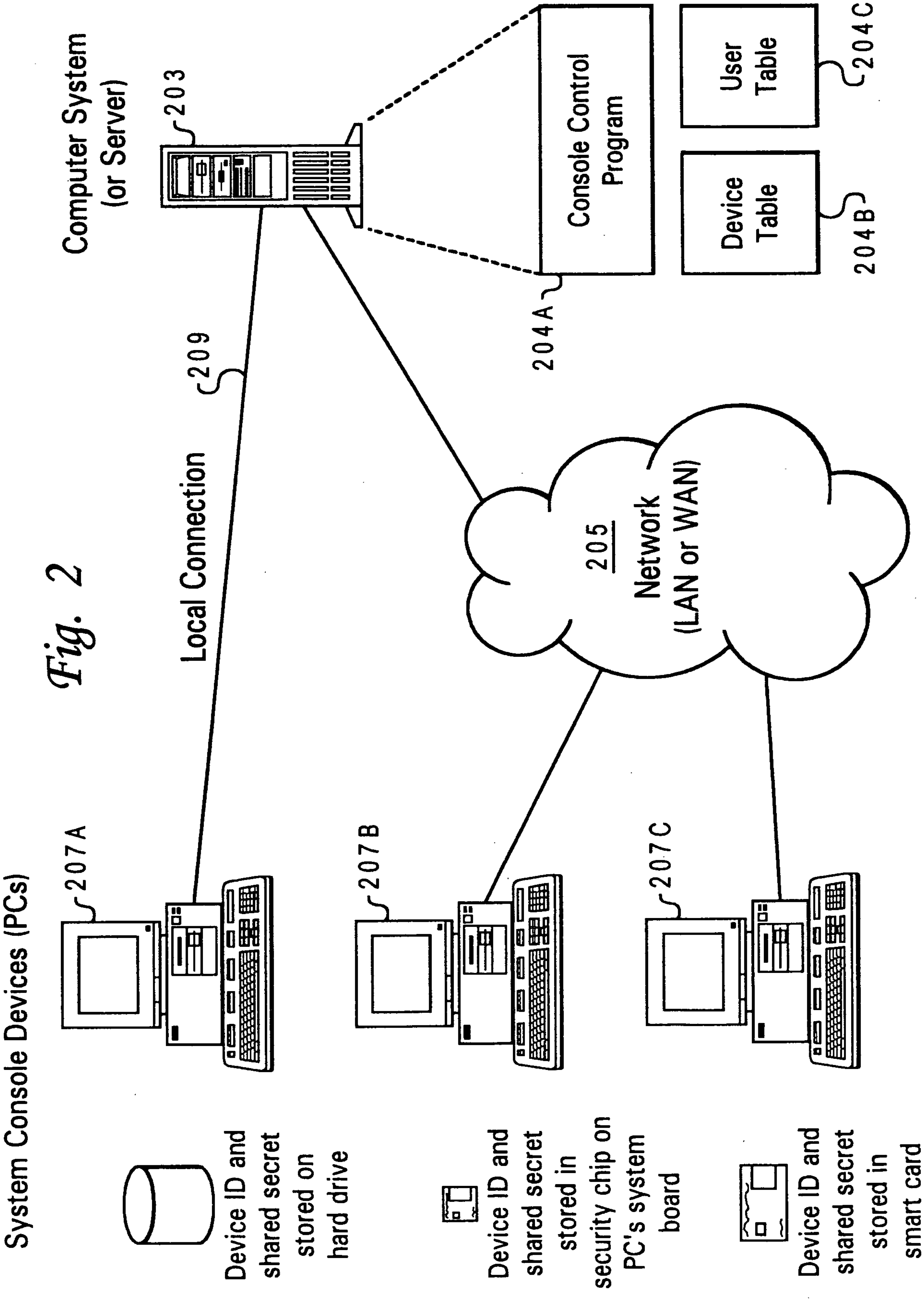
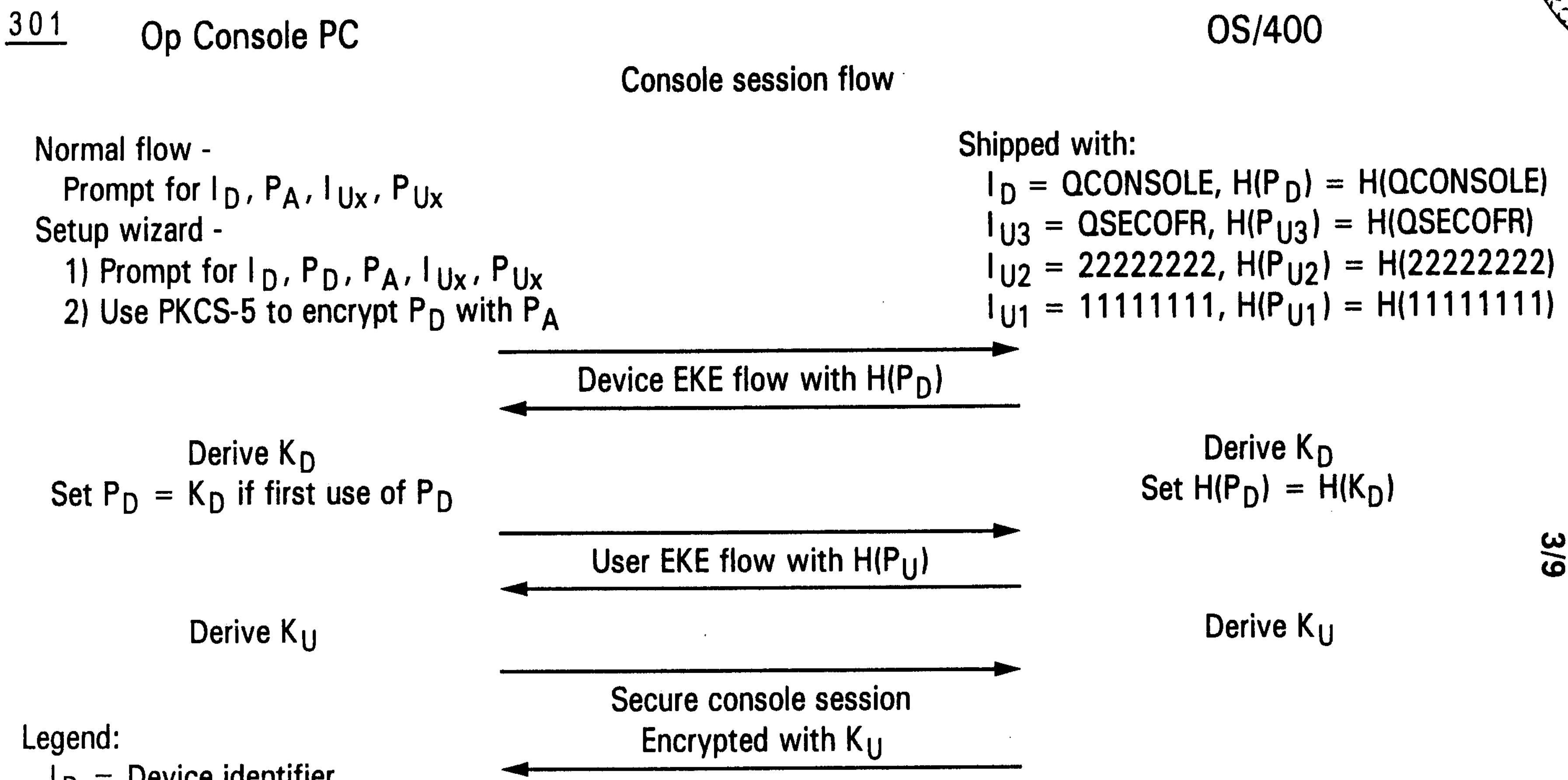


Fig. 2

System Console Devices (PCs)
207A
207B
207C
Device ID and shared secret stored on hard drive
Device ID and shared secret stored in security chip on PC's system board
Device ID and shared secret stored in smart card
Local Connection
209
Computer System (or Server)
203
205
Network (LAN or WAN)
Console Control Program
204A
Device Table
204B
User Table
204C


301
Op Console PC
OS/400
Console session flow
Normal flow -
Prompt for I_D, P_A, I_{Ux}, P_{Ux}
Setup wizard -
1) Prompt for I_D, P_D, P_A, I_{Ux}, P_{Ux}
2) Use PKCS-5 to encrypt P_D with P_A
Shipped with:
I_D = QCONSOLE, $H(P_D)$ = H(QCONSOLE)
I_{U3} = QSECOFR, $H(P_{U3})$ = H(QSECOFR)
I_{U2} = 22222222, $H(P_{U2})$ = H(22222222)
I_{U1} = 11111111, $H(P_{U1})$ = H(11111111)
Device EKE flow with $H(P_D)$
Derive K_D
Set $P_D = K_D$ if first use of P_D
Derive K_D
Set $H(P_D) = H(K_D)$
User EKE flow with $H(P_U)$
Derive K_U
Derive K_U
Secure console session
Encrypted with K_U

Legend:
I_D = Device identifier
P_D = Device shared secret
P_A = Access passphrase
I_{Ux} = User ID
P_{Ux} = User passphrase
K_D = Device session key
K_U = User session key
R = Random number
H(x) = Hash of x

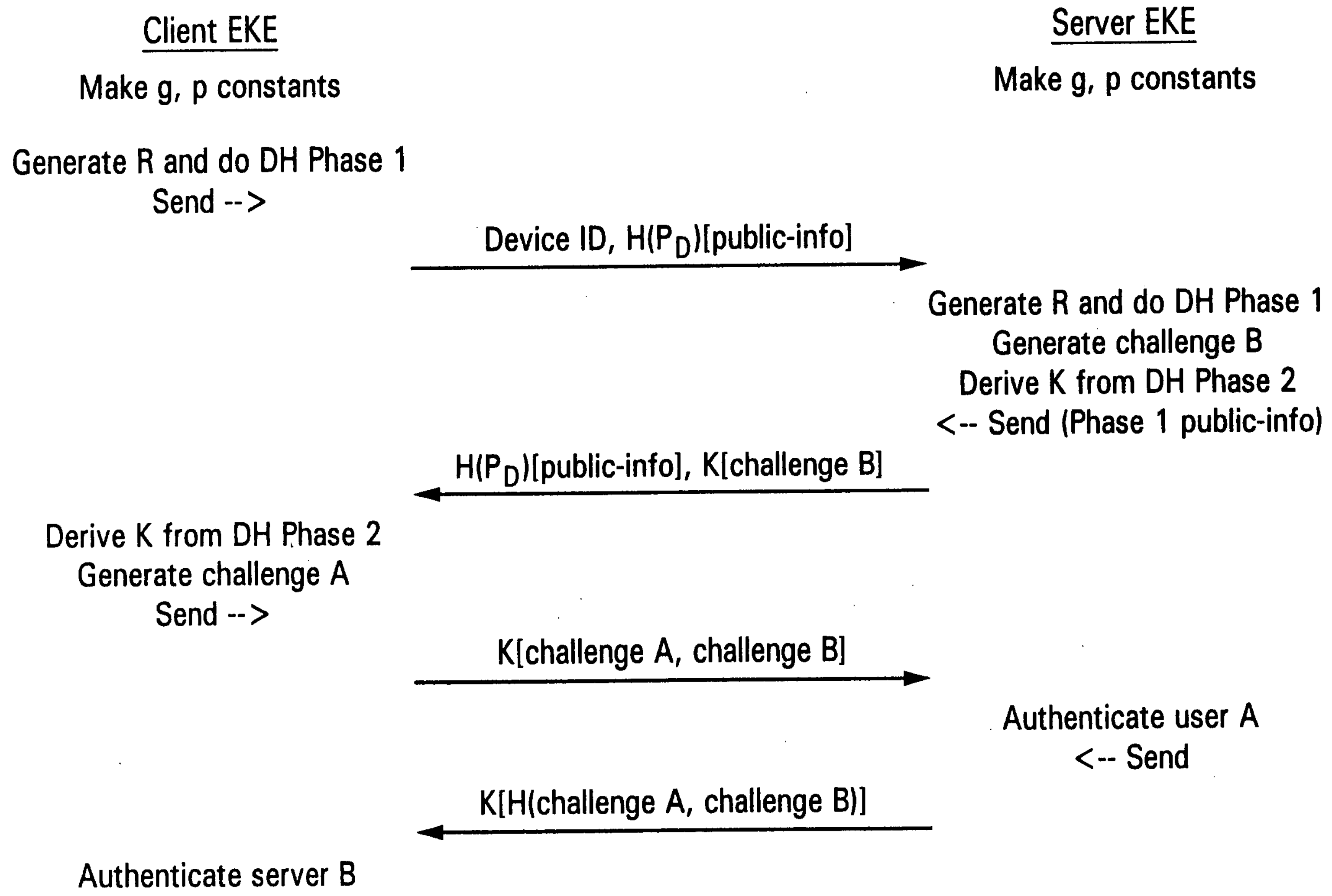
NOTE: The first console session uses the well known shipped device identifier and user ID to access the iSeries. The device passphrase is modified in the initial flow ($P_D = K_D$). Therefore, the genesis device essentially "gets in free."

Fig. 3A

Fig. 3B

303

- Generate DH parameters g and p
- Where g = base; p = prime; these values do not have to be secret (public-info)
- Make g and p constants in server and client EKE code



Client EKE

Make g, p constants

Generate R and do DH Phase 1
Send -->

Server EKE

Make g, p constants

Device ID, $H(P_D)$[public-info]

Generate R and do DH Phase 1
Generate challenge B
Derive K from DH Phase 2
<-- Send (Phase 1 public-info)

$H(P_D)$[public-info], K[challenge B]

Derive K from DH Phase 2
Generate challenge A
Send -->

K[challenge A, challenge B]

Authenticate user A
<-- Send

K[H(challenge A, challenge B)]

Authenticate server B

Refer to BSAFE Reference Manual for description of DH Phase 1 & 2.
NOTE: The challenge strings must be a different length than the encryption block.

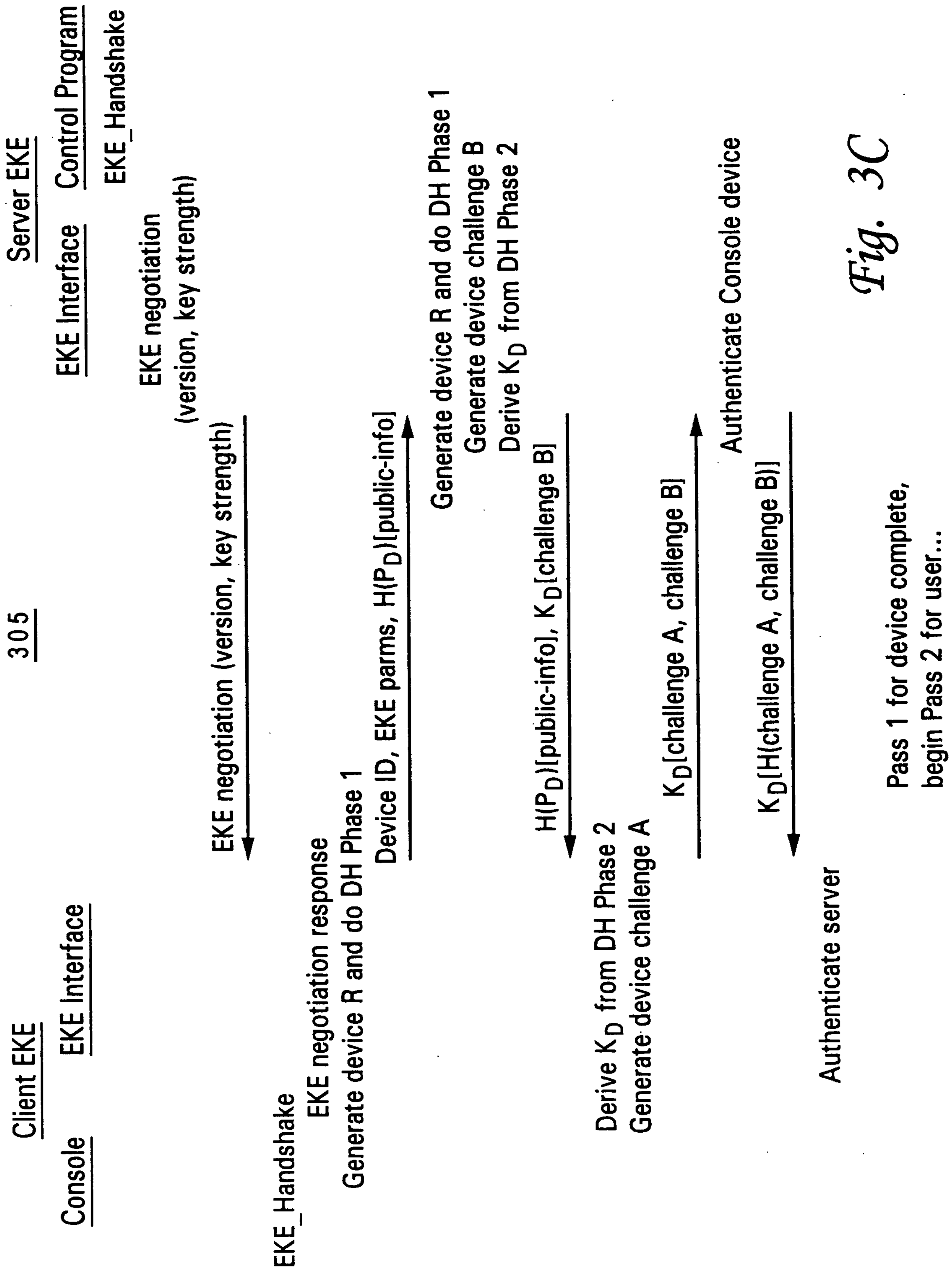
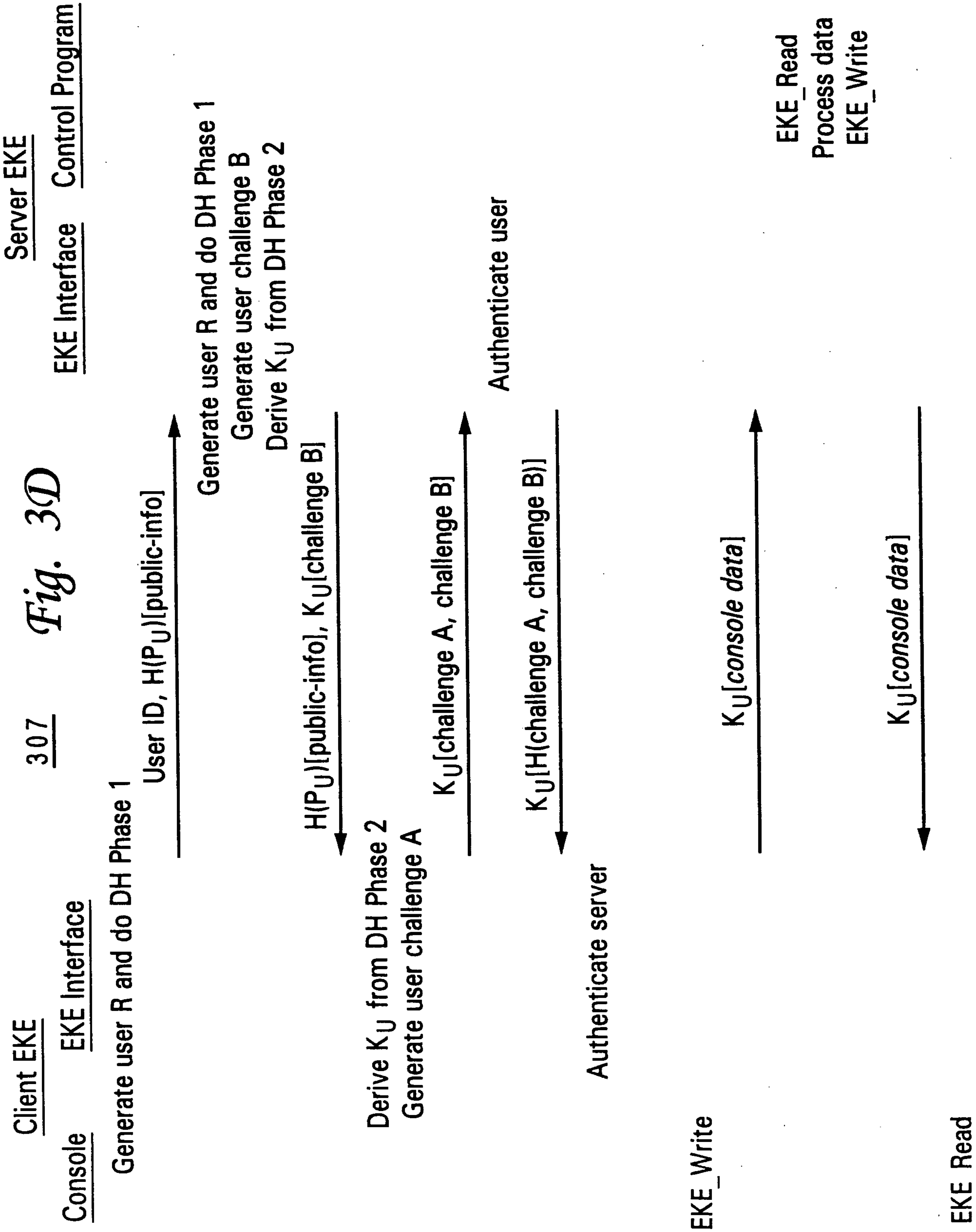

Client EKE
Console
EKE Interface
305
Server EKE
EKE Interface
Control Program
EKE_Handshake
EKE negotiation
(version, key strength)
EKE negotiation (version, key strength)
EKE_Handshake
EKE negotiation response
Generate device R and do DH Phase 1
Device ID, EKE parms, H(P_D)[public-info]
Generate device R and do DH Phase 1
Generate device challenge B
Derive K_D from DH Phase 2
H(P_D)[public-info], K_D[challenge B]
Derive K_D from DH Phase 2
Generate device challenge A
K_D[challenge A, challenge B]
Authenticate Console device
K_D[H(challenge A, challenge B)]
Authenticate server
Pass 1 for device complete,
begin Pass 2 for user...

Fig. 3C


Client EKE
Console
EKE Interface
Server EKE
EKE Interface
Control Program
Generate user R and do DH Phase 1
User ID, H(P_U)[public-info]
Generate user R and do DH Phase 1
Generate user challenge B
Derive K_U from DH Phase 2
H(P_U)[public-info], K_U[challenge B]
Derive K_U from DH Phase 2
Generate user challenge A
K_U[challenge A, challenge B]
Authenticate user
K_U[H(challenge A, challenge B)]
Authenticate server
EKE_Write
K_U[console data]
EKE_Read
Process data
EKE_Write
K_U[console data]
EKE_Read

307

Fig. 3D

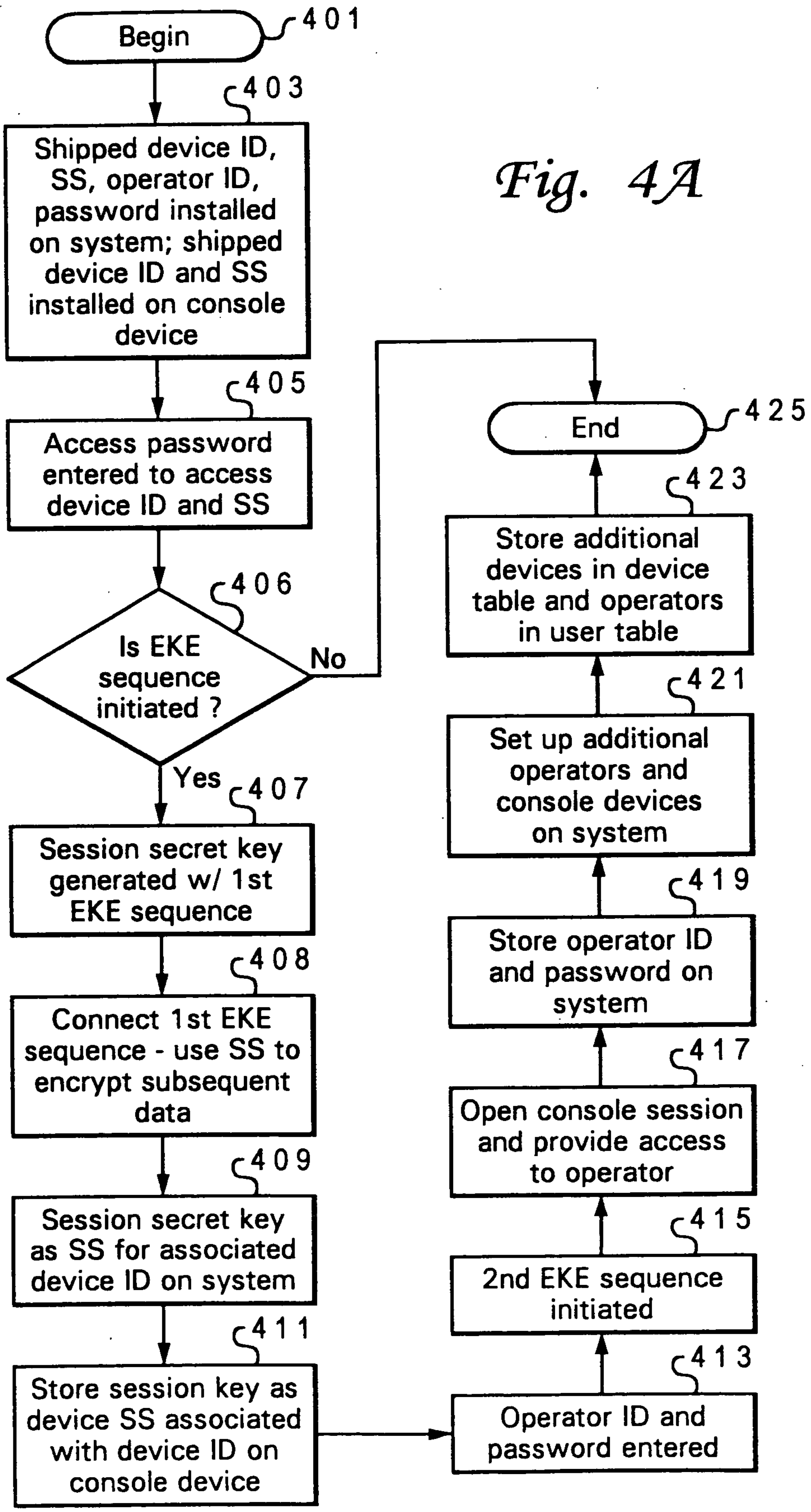

Begin
401
403
Shipped device ID, SS, operator ID, password installed on system; shipped device ID and SS installed on console device
405
Access password entered to access device ID and SS
406
Is EKE sequence initiated ?
No
Yes
407
Session secret key generated w/ 1st EKE sequence
408
Connect 1st EKE sequence - use SS to encrypt subsequent data
409
Session secret key as SS for associated device ID on system
411
Store session key as device SS associated with device ID on console device
413
Operator ID and password entered
415
2nd EKE sequence initiated
417
Open console session and provide access to operator
419
Store operator ID and password on system
421
Set up additional operators and console devices on system
423
Store additional devices in device table and operators in user table
End
425

Fig. 4A

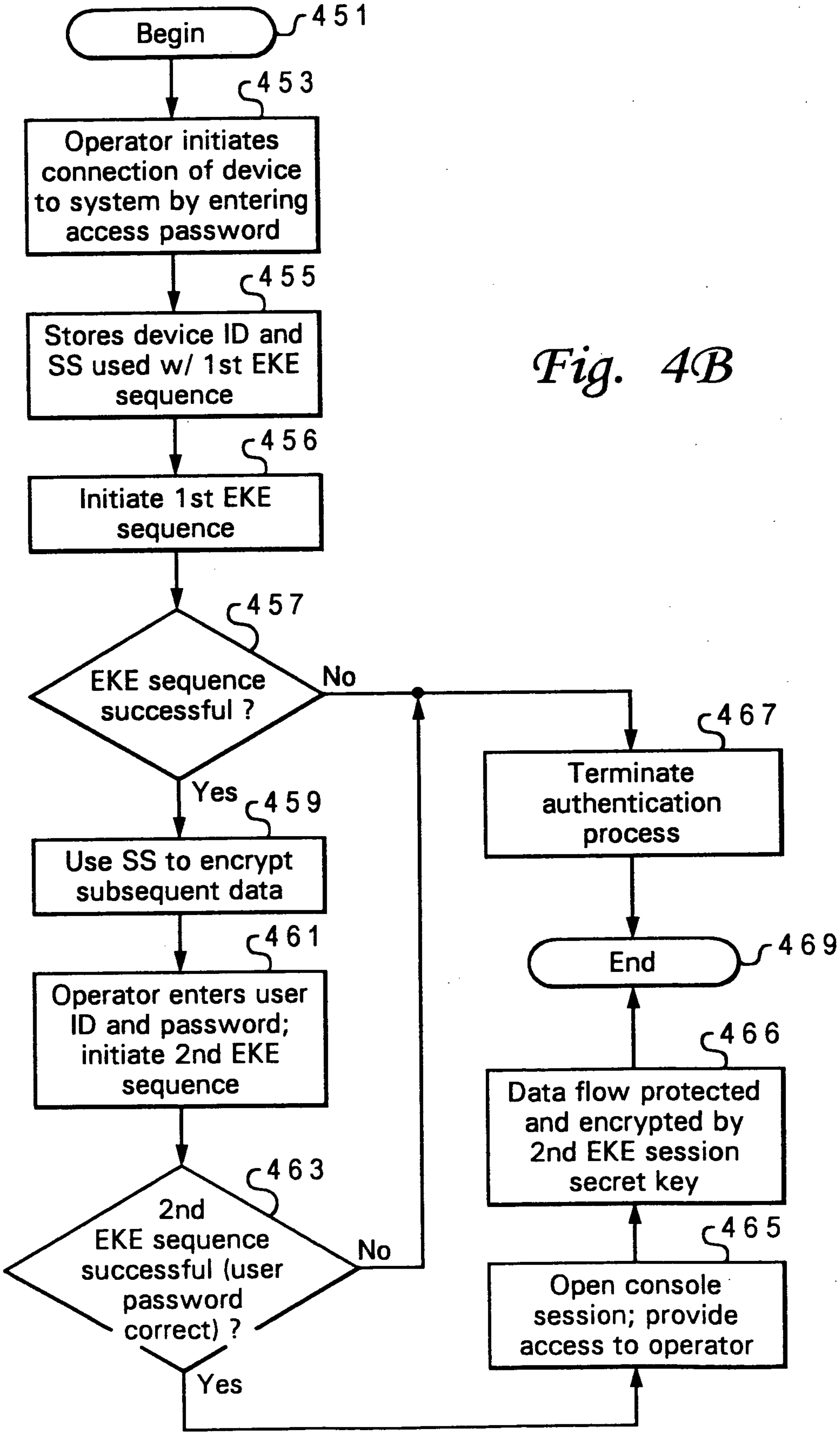

Begin
451
Operator initiates connection of device to system by entering access password
453
Stores device ID and SS used w/ 1st EKE sequence
455
Initiate 1st EKE sequence
456
EKE sequence successful ?
457
No
Yes
Use SS to encrypt subsequent data
459
Operator enters user ID and password; initiate 2nd EKE sequence
461
2nd EKE sequence successful (user password correct) ?
463
No
Yes
Terminate authentication process
467
End
469
Data flow protected and encrypted by 2nd EKE session secret key
466
Open console session; provide access to operator
465

Fig. 4B

Client Device (PC) 501

Server Connection	
Server1	Hash (device identifier, shared secret)
Server2	Hash (device identifier, shared secret)

Fig. 5A

Server

Device Table 511

Device Identifier	Hashed shared secret
QCONSOLE	H(shared secret)
DEVICE2	H(shared secret)

User Table 513

User Identifier	Hashed password
11111111	H(password)
22222222	H(password)
QSRV	H(password)
QSECOFR	H(password)

Fig. 5B